

UNITED STATES DISTRICT COURT

WESTERN

for the
DISTRICT OF

OKLAHOMA

FILED

IN THE MATTER OF THE SEARCH OF CONTENT OF)
AND RECORDS RELATING TO EMAIL AND/OR iCloud)
ACCOUNTS:)

tjohnsontsg@icloud.com, niaforte360@icloud.com,)
tjohnstontsg@me.com,)
Laura R. Johnson)
8033 NW 124th Street)
Oklahoma City, OK 73142-2232)
Telephone number (405) 641-4016)

IN THE POSSESSION OF AND MAINTAINED AT:)

Apple, Inc.)
1 Infinite Loop)
Cupertino, CA 95014)

NOV - 9 2018

CARMELO A REEDER SHIN
CLERK U.S. DISTRICT COURT
BY Carrie Sims
DEPUTY

Case No.

M-18-555-P

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (check one or more):

- ☒ evidence of the crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1341
18 U.S.C. § 1343
18 U.S.C. § 1344
18 U.S.C. § 1957
18 U.S.C. § 1028(a)(7)
18 U.S.C. § 371
18 U.S.C. § 1028A
18 U.S.C. § 371

Offense Description

Mail Fraud;
Wire Fraud;
Bank Fraud;
Money Laundering;
Identity Theft;
Conspiracy to Commit Identity Theft;
Aggravated Identity Theft
Conspiracy to Commit Aggravated Identity Theft

The application is based on these facts:

See attached Affidavit of Special Agent Kimberly Carter, United States Secret Service, which is incorporated by reference herein.

- ☐ Continued on the attached sheet(s).
☐ Delayed notice of _____ days (give exact ending date if more than 30 days) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).



Applicant's signature

Kimberly Carter
Special Agent
United States Secret Service

Sworn to before me and signed in my presence.

Date: 11/9/18

City and State: Oklahoma City, Oklahoma



Judge's signature

GARY M. PURCELL, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

PLACE TO BE SEARCHED

This warrant applies to content of and information about the following accounts:

- a. tjohnsontsg@me.com
- b. tjohnsontsg@icloud.com
- c. niaforte360@icloud.com
- d. any iCloud account associated with:

Laura R. Johnson
8033 NW 124th Street
Oklahoma City, OK 73142-2232
Telephone number (405) 641-4016

that are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

A handwritten signature in black ink, appearing to be "J. B. Koe", is located in the bottom right corner of the page.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc., regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to Apple, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. The contents of all emails associated with the accounts from January, 2014 until April, 2018, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each

A handwritten signature in black ink, appearing to be "J. Smith" or similar, with a stylized flourish at the end.

email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

c. The contents of the following files and other records stored on iCloud: all iOS device backups, and all files and other records related to iCloud Mail.

d. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including mail logs, iCloud logs, and iTunes Store logs.

e. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

f. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

A handwritten signature in black ink, located in the bottom right corner of the page. The signature is stylized and appears to read "Jab" followed by a date "11/9".

AFFIDAVIT

1. I, Kimberly Carter, am a Special Agent employed by the United States Secret Service (Secret Service). I have been employed by the Secret Service for over 21 years. I am currently assigned to the Oklahoma City office of the Secret Service where I am responsible for the investigation of Title 18, United States Code, offenses including white collar criminal offenses.

2. As a Secret Service agent, I have conducted numerous criminal investigations, assisted in the execution of search and arrest warrants, conducted physical surveillance, analyzed records, and interviewed witnesses as well as suspects. The facts and information set forth in this affidavit are derived from an investigation conducted by the Secret Service and the Consumer Protection Unit of the Oklahoma Attorney General's Office.

3. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to investigators. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

4. This affidavit is offered in support of an application for a search warrant in the Western District of Oklahoma for information about and content of email accounts that are stored at premises owned, controlled, maintained, or operated by Google, Inc., an email provider which is headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

5. This affidavit is also offered in support of an application for a search warrant in the Western District of Oklahoma for information about and content of email and iCloud accounts that are stored at premises owned, controlled, maintained, or operated by Apple, Inc., a company headquartered at 1 Infinite Loop, Cupertino, CA.

6. As to both of the warrants sought, the information to be searched is described in the following paragraphs and in Attachments A and B.

7. As to both of the warrants sought, this affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, this Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

9. Based upon the information contained in this affidavit, I submit that probable cause exists to believe that:

- a. One or more persons, including Cheryl Ashley, Laura R. Johnson and Thomas C. Johnson, Sr., have devised a scheme to defraud and to obtain money and property by means of false or fraudulent representations and have knowingly executed and caused the execution of the scheme through the use of the United States mail in violation of Title 18, United States Code, Section 1341;
- b. One or more persons, including Cheryl Ashley, Laura R. Johnson and Thomas C. Johnson, Sr., have devised a scheme to defraud and to obtain money and property by means of false or fraudulent representations and have knowingly caused the wire transmission of documents in interstate commerce in violation of Title 18, United States Code, Section 1343;

- c. One or more persons, including Laura R. Johnson and Thomas C. Johnson, Sr., have knowingly executed and attempted to execute a scheme to defraud and to obtain money under the custody of a financial institution in violation of Title 18, United States Code, Section 1344;
- d. One or more persons, including Laura R. Johnson and Thomas C. Johnson, Sr., have knowingly engaged in a monetary transaction in criminal derived property of a value greater than \$10,000 where the money was the proceeds of bank fraud in violation of Title 18, United States Code, Section 1957;
- e. One or more persons, including Cheryl Ashley, Laura R. Johnson and Thomas C. Johnson, Sr., have knowingly transferred, possessed or used, without lawful authority, a means of identification of another person with the intent to commit or aid and abet in the commission of a federal offense of mail fraud and/or wire fraud, or a State of Oklahoma offense of procuring or offering a false instrument to be filed in a public office (21 OSA 463), in violation of Title 18, United States Code, Section 1028(a)(7);
- f. Two or more persons, including Cheryl Ashley, Laura R. Johnson and Thomas C. Johnson, Sr., have knowingly conspired in violation of Title 18, United States Code, Section 371, to transfer, possess or use, without lawful authority, a means of identification of another person with the intent to commit or aid and abet in the commission of a federal offense of mail fraud and/or wire fraud, or a State of Oklahoma offense of procuring or offering a false instrument to be filed in a public office (21 OSA 463), in violation of Title 18, United States Code, Section 1028(a)(7);
- g. One or more persons, including Cheryl Ashley, Laura R. Johnson and Thomas C. Johnson, Sr., knowingly transferred, possessed or used, without lawful authority, a means of identification of another person to commit mail fraud, wire fraud or bank fraud under Title 18, United States Code, Section 1028A.
- h. Two or more persons, including Cheryl Ashley, Laura R. Johnson and Thomas C. Johnson, Sr., knowingly conspired in violation of Title

18, United States Code, Section 371, to transfer, possess or use, without lawful authority, a means of identification of another person to commit mail fraud, wire fraud or bank fraud under Title 18, United States Code, Section 1028A.

SUMMARY OF INVESTIGATION

10. The United States Secret Service and the Consumer Protection Unit of the Oklahoma Attorney General's Office are conducting a criminal investigation of individuals who have fraudulently obtained and attempted to obtain title to real properties located in the Western District of Oklahoma through the use of forged warranty and quit claim deeds, forged documents, forged notaries' signatures and seals, as well as false eviction notices. At this time, I have identified at least 15 properties that appear to have been targeted for takeover in this warranty deed fraud. I do not represent these are the only homes targeted by individuals involved in this warranty deed fraud as there may well be other properties that have not yet been identified.

11. Delinquent property taxes were owed on many of the properties. Individuals involved in this fraud appear to target such properties, pay at least one year of the back taxes, create and file forged deeds and then claim to have purchased the properties through county tax auctions. However, investigators have determined the properties fraudulently taken over by individuals in this fraud have not been auctioned by county officials for delinquent taxes. Additionally, I know that Cheryl Ashley and her daughter Laura R. Johnson are aware of the actual procedures used by county officials to auction properties. In fact, both women have successfully bid on properties auctioned by Oklahoma County. In addition to properties owing delinquent property taxes, at least one property targeted by

these individuals had been involved in a foreclosure suit.

12. During the course of this investigation, another investigator and I have examined numerous deeds and court documents and have spoken with some homeowners or their lawyers regarding the fraudulent actions taken against their properties. The property owners and lawyers who have been interviewed stated the owners had not signed the deeds transferring their properties and that their names had been forged.

13. I believe the signatures and seals of numerous notaries have been forged or fraudulently scanned onto these deeds to give the appearance of a legitimate title transaction. Not all notaries whose names appear on these documents have been interviewed. However, over 15 notaries have been interviewed who stated that the seals and signatures on the deeds and on other documents are not their own and that they had not notarized the documents. A lawyer for a company that employs one notary, whose signature and seal appears on two documents, advised an investigator that the notary notarized one document but a second document with her notary seal and signature was a forgery.

14. In some cases, individuals involved in this warranty deed fraud have successfully taken over properties. For example, Dru Hayhurst received a notice from the Oklahoma Treasurer's Office that unless he paid delinquent property taxes on his home at 2728 Cambridge Court in Oklahoma City, the county would auction the property to pay back taxes. Hayhurst immediately paid all of the back taxes on line. After payment of his property taxes, Hayhurst received a false eviction notice purportedly signed by former Oklahoma County Sheriff John Whetsel. Hayhurst believed he had been too late in paying

the delinquent taxes and simply walked away from his home when he received the eviction notice. Hayhurst's home had been completely paid off. On February 23, 2017, a warranty deed allegedly signed by Hayhurst on August 2, 2016, transferring his home to OT LLC was filed with the Oklahoma County Clerk's Office. Hayhurst stated he did not sign any deed transferring his property.

15. Some homeowners, whose property was affected by this fraud, hired attorneys to file quiet title actions in the Oklahoma district courts. The individuals involved in this warranty deed scam have fought those quiet title actions. One example involves the attempted takeover of a home located in Oklahoma County and owned by Lucinda Giovanni, who at the time resided in California.

**The Attempted Takeover of Lucinda Giovanni's Home
10204 Major Avenue, The Village**

16. In 2016, Lucinda Giovanni lived in California but owned a home at 10204 Major Avenue in the Village, located in Oklahoma County. In 2016, Giovanni received a notice from the Oklahoma County Treasurer's Office that her home would be put up for auction due to delinquent taxes.

17. Giovanni contacted a friend, Norma Funston, who paid the 2012 property taxes on the home in May of 2016. A county employee told Funston the property would not be auctioned because of the payment of the 2012 taxes. Giovanni's brother, Bruce Ball, who lives in Oklahoma City, periodically checked on the home. In June of 2016, Ball met a man who identified himself as Keith Burkhart standing near the door to Giovanni's home. Burkhart asked Ball if he was the locksmith.

18. Burkhart said he represented a Las Vegas company called Help and Hope that had purchased the home at a tax sale. Funston arrived at the home, showed the man the receipt of her payment for the 2012 delinquent taxes and told him the Treasurer's Office stated the home would be withdrawn from the tax sale. Burkhart refused to provide any contact information for Help and Hope.

19. Funston re-contacted the Treasurer's office which confirmed the house had been withdrawn from the auction. Funston was also told that someone else had paid the 2013, 2014 and 2015 property taxes on the home. Oklahoma County Treasurer's Office records show that in June 2016, a company called Help and Hope LLC, 10252 Highland Gardens Drive in North Las Vegas, Nevada had paid delinquent taxes for those three years.

20. Giovanni subsequently received a letter from Help and Hope LLC in the mail at her California address. The letter claimed Help and Hope had purchased her home at a tax sale but would sell it back to her for \$13,500. The letter was signed by "Nia Forte" and listed a phone number of (405) 234-6151 and an email address of niaforte360@gmail.com. If Giovanni didn't want to buy back her property, the letter stated she could sign an enclosed warranty deed form transferring the property to Help and Hope LLC and return it to Forte. Giovanni did not accept either option. Your affiant has reviewed a copy of the letter and the warranty deed form sent to Giovanni.

**The Takeover of Lucinda Giovanni's Home
10204 Major Avenue, The Village**

21. On April 17, 2017, approximately ten months after Giovanni received the letter from Help and Hope LLC, a warranty deed allegedly signed by Giovanni on June 12, 2016, was filed with the Oklahoma County Clerk's Office. The deed purportedly conveyed the home at 10204 Major Avenue, from Giovanni to OT LLC. The deed shows Giovanni's signature was notarized by Deborah Abbott, who is a licensed notary in Oklahoma. After reviewing this deed, Giovanni stated the signature on the warranty deed was a forgery and that she did not convey her home to anyone. Abbott also reviewed this deed and stated she did not sign or notarize the warranty deed nor did she place her seal on the document.

22. On June 27, 2017, a second warranty deed on Giovanni's property was filed with the Oklahoma County Clerk's Office. This deed purports to have been signed on February 12, 2017, by "Arianna Jones" as a managing member of OT LLC, and transferred the property to Helping Hand LLC.

23. Additionally, on June 27, 2017, a mortgage between "The Texas Bank" and Helping Hand LLC was filed on Giovanni's home at 10204 Major Avenue. The mortgage document listed the address of the Texas Bank as being 5830 NW Expressway #178, Oklahoma City, OK 73132, which is a private postal box at a UPS store. This UPS box was opened on June 27, 2017, by Cheryl Ashley. The name of the corporation listed on this form is Helping Hand LLC.

24. During the course of this investigation, a representative of The Texas Bank stated the bank had no interest in Giovanni's property, did not have a physical presence in Oklahoma, nor did it receive mail at 5830 NW Expressway #178.

**The Quiet Title Court Case
10204 Major Avenue, The Village**

25. A quiet title civil lawsuit was filed by Giovanni on June 30, 2017, in Oklahoma County District Court. The lawsuit lasted several months and resulted in a journal entry of judgment for Giovanni on November 17, 2017, against all defendants including OT LLC, Helping Hand LLC and Arianna Jones.

26. During the course of the lawsuit, a Special Entry of Appearance and Motion to Dismiss was filed July 17, 2017, on behalf of the defendants by The Crossanall Firm and signed by George Crossanall, #21895, of 208 Fountainview Drive, Euless Texas. In the pleading, Crossanall claimed OT LLC legally obtained Giovanni's home after suing her in small claims court in California where it won a judgment of \$32,248.52 against her. Crossanall attached "Exhibit A," entitled "SC-200 Notice of Entry of Judgment" which he represented to be the small claims judgment against Giovanni and in favor of OT LLC.

27. I believe this document is fictitious. First, Giovanni has stated she was never the subject of such small claims lawsuit. Second, several areas on the California small claims judgment, marked "Exhibit A," have been "blacked out" including the case number for the lawsuit. Third, the website for the California court system provides general information about suing in small claims court. Specifically "SC-100-Info" provides information for a small claims plaintiff including the fact that a small claims court in

California cannot award a judgment for more than \$5,000 to a business. Furthermore, if a business files a claim for more than the maximum allowable amount, it gives up the right to collect any amount over the \$5,000 limit. Fourth, the California court form, “SC-200 Notice of Entry of Judgment” is an interactive form that can be accessed electronically through the Internet, filled out on line and printed. Finally, both the Texas Bar Association and the Oklahoma Bar Association have confirmed that George Crossanall is not a licensed attorney in either Texas or Oklahoma.

28. Giovanni’s quiet title lawsuit was successful as the district court judge found the deeds conveying the property were forgeries and vacated the mortgage.

**Jewel Marvine Bartrug
5636 NW 58th Terrace, Warr Acres**

29. In at least one case, a home involved in this warranty deed fraud was taken over four years after the homeowner had died. Jewel Marvine Bartrug and her husband purchased their home at 5636 NW 58th Terrace in Warr Acres in 1981. Bartrug remained in the home after her husband died until her death in June 2012.

30. Bartrug was discovered dead in her home on June 24, 2012, by a neighbor checking on her welfare. Her body was transported to the Oklahoma County Medical Examiner’s Office where it remained unclaimed. On August 16, 2012, the medical examiner’s office released Bartrug’s body to Demuth Funeral Home where she was cremated on August 22, 2012.

31. After Bartrug’s death, the property taxes on her home became delinquent. Oklahoma County records show the 2011 back taxes on Bartrug’s property were paid in

cash on June 5, 2015. Payment for delinquent taxes for 2012 through 2014 were made on June 22, 2015 using Money Grams.

32. I believe Laura R. Johnson and her husband, Thomas C. Johnson Sr., gained entry into Bartrug's home no later than in July of 2016, based upon their accessing Bartrug's three bank accounts at MidFirst Bank where she had approximately \$170,000. On July 25, 2016, Thomas C. Johnson Sr., deposited an \$8,000 check signed "Marvine Bartrug" and drawn on her MidFirst Bank account x6767 into his Showtech Distributors (Showtech) account x3701 at the Bank of Oklahoma (BOK). The next day he deposited a \$22,000 check signed "Marvine Bartrug" and drawn on the same MidFirst Bank account into his Showtech account. Both checks were made payable to Help and Hope. Prior to the deposit of the two Bartrug checks, the Showtech account had a balance of \$320.57.

33. Although both checks were returned by MidFirst Bank to the Bank of Oklahoma, Thomas C. Johnson Sr., had already withdrawn approximately \$23,000 from the Showtech account. When contacted by a BOK investigator about the checks, Thomas C. Johnson Sr., said Bartrug had written the checks for equipment she purchased for her church. Only after the BOK investigator confronted him with Laura R. Johnson's use of a power of attorney for Bartrug, did Thomas C. Johnson Sr., admit he knew Bartrug was dead when he presented the checks with Bartrug's purported signature.

34. In July of 2016, Laura R. Johnson went to MidFirst Bank where she presented a Power of Attorney form supposedly signed by Bartrug that gave Johnson power to handle Bartrug's affairs. MidFirst Bank required a power of attorney checklist be filled

out that described the purpose for the withdrawal and why Bartrug was unable to perform the transaction herself.

35. Laura R. Johnson stated she needed \$10,000 to fix Bartrug's teeth and that Bartrug wanted to prepay Help and Hope LLC for up to two years of care. She also stated that Bartrug could not perform this financial action on her own because she "is physically fragile." Bartrug died in June 2012.

36. Laura R. Johnson and Thomas C. Johnson Sr., continued to cause money to be withdrawn from Bartrug's accounts at MidFirst Bank. Approximately \$75,000 was withdrawn between July 19, 2016 and October 17, 2016 for the benefit of the Johnsons. These withdrawals included two separate automated clearing house (ACH) withdrawals of \$10,962.24 paid towards the Johnsons' home mortgage and three ACH transactions totaling over \$16,000 for payment on a Discover account for Thomas C. Johnson Sr.

37. The Oklahoma County Clerk's Office records show two transactions recorded on Bartrug's home on October 25, 2016. First, an "Affidavit of Surviving Joint Tenant" allegedly signed on January 4, 2012, by Laura R. Johnson, as attorney in fact for Bartrug, was filed at 8:06:29 a.m. on October 25, 2016. This document allegedly was notarized by Kathy Griffith, who is a licensed notary in Oklahoma. Griffith has reviewed this document and told investigators she did not sign or notarize this document.

38. Second, a warranty deed allegedly signed on May 11, 2012 by Laura Renee Johnson, as attorney in fact for Bartrug, transferring the property to Innovative Transformations Inc., was filed at 8:06:30 a.m. on October 25, 2016. This document shows Laura Renee Johnson's signature was notarized by Tracy Putman, who is a licensed notary

in Oklahoma. Putman has reviewed this document and told investigators she did not sign or notarize this document.

39. On November 8, 2017, a warranty deed allegedly signed July 18, 2016, by an officer of Innovative Transformations Inc., transferred Bartrug's home to the Family Heritage Trust. This deed was filed with the Oklahoma County Clerk's Office on November 8, 2017.

40. The October 25, 2016, title transactions occurred approximately two weeks after Bartrug's nephew, Charles Bartrug, filed a petition to handle his deceased aunt's estate on October 7, 2016, in Oklahoma County probate court. On November 1, 2016, Laura R. Johnson contested Charles Bartrug's request to handle the estate, claiming she possessed the "Last Will and Testament of Jewel M. Bartrug," which left the entire estate to her.

41. I believe the "Last Will and Testament of Jewel M. Bartrug" is a fraudulent document. First, this Last Will allegedly signed by Bartrug on January 4, 2012, and witnessed by "Nia Forte" and "Keith Barrett," purports to have been notarized on that same date by Kathy Griffith. Griffith reviewed this document and stated she did not sign or notarize the document.

42. Second, in July of 2016, Laura R. Johnson represented to MidFirst Bank that she needed to withdraw money from Bartrug's bank accounts to fix Bartrug's teeth and to pay for ongoing care by Help and Hope over the next two years. She also told MidFirst bank that Bartrug could not conduct the withdrawals herself because she "is physically

fragile” which clearly represented that Bartrug was alive in 2016, when in fact she died in 2012.

43. Third, Nia Forte is a name used elsewhere in this fraudulent warranty deed scheme. Specifically, Forte is the representative of Help and Hope who sent a letter to Giovanni offering to allow Giovanni to pay \$13,500 to buy her home back. In that letter to Giovanni, Forte listed her phone number as (405) 234-6151. This telephone number is associated with a Verizon prepaid telephone number activated on June 15, 2016, in the name of Jewel Bartrug, who died nearly four years earlier.

44. Fourth, Renew Contractors LLC, on July 6, 2016, filed a “notice of interest” against Giovanni in her quiet title lawsuit and listed (405) 234-6151 as the company’s phone number.

45. Finally, the name “Keith Barrett” appears on a number of documents, as an agent for Enginuity LLC, a Nevada company associated with Thomas C. Johnson, Sr. In documents filed in an unrelated matter, Johnson is listed as the CIO for Enginuity and lists the address of 8033 NW 124th, Oklahoma City, which is the home of Laura Johnson and Thomas C. Johnson Sr.

46. Eventually, Charles Bartrug dismissed his petition in probate court.

Bruce Willson
10407 Ridgeview Drive, The Village

47. I am aware that the Village Police Department became involved in an investigation of an attempted property takeover of the home of Bruce Willson in the Village by individuals in this warranty deed fraud. On July 20, 2017, Village Police officers

responded to a call regarding individuals who claimed to have purchased Willson's home and were attempting to make him leave. Willson told the police officers a deed had been filed transferring his property but that he had not signed such a deed.

48. Lt. B. South spoke with a woman who identified herself as "Carol Mary Ashton" and stated she worked for a company that purchased the house. "Ashton" stated she was there to clean up the yard so that it could be sold. When asked the name of the company, "Ashton" stated she couldn't remember the name because she worked for five different companies. "Ashton" later changed her story stating she had paid the back taxes on the house which was part of the deal when she bought the house. "Ashton" was unable to produce any identification but did give her telephone number as (405) 388-0683. Village police later identified this phone number as belonging to Cheryl Mary Ashley.

49. Lt. Smith was aware of an ongoing mortgage fraud scheme in the Village and contacted Village Police Detective Frazier to discuss the case. While Lt. Smith was on the phone with Frazier, "Ashton," an adult male and two children drove away from the home. Through public records, Village police determined the woman was Cheryl M. Ashley and the adult male who had been at the home was Cheryl Ashley's son, Raymond Michael Ashley.

**Janice and Joe Shorter
8825 Parkridge Terrace, Oklahoma City**

50. On January 27, 2014, the Mortgage Clearing Corporation filed a foreclosure action against Janice and Joe Shorter because they had defaulted on a promissory note on the home. The Shorters had moved into a nursing home due to strokes suffered by Joe

Shorter. On April 30, 2014, a journal entry of judgment in the total amount of approximately \$13,000 plus interest was entered against the Shorters. A sheriff's sale was ordered to pay off the judgment and to place any amount in excess of the judgment into the Court Clerk's Office fund until further order.

51. On July 22, 2014, the Shorters' home appraised for \$110,000. At the November 11, 2014 sheriff's sale, Cheryl Ashley submitted the highest bid of \$77,000 which was accepted. On September 12, 2014, Oklahoma County Court Clerk records show that Cheryl Ashley deposited \$3,000 and an entity called Parkridge LLC deposited \$4,700 into the Court Clerk's Office for the property.

52. The hearing to confirm the sale of the Shorters' home to Cheryl Ashley was scheduled for October 3, 2014. Cheryl Ashley failed to appear at the hearing and failed to deposit the remainder of the purchase price into the court clerk's fund.

53. However, a warranty deed, allegedly signed by the Shorters on September 29, 2014, transferring their home to Showtech Distributors LLC was filed with the Oklahoma County Clerk's Office on October 3, 2014. This deed was notarized by Cheryl Ashley. A second warranty deed filed October 16, 2014, with the Oklahoma County Clerk's Office, transferred the Shorters' home from Showtech Distributors to Help and Hope LLC.

54. On November 7, 2014, court records show Help and Hope LLC paid an additional \$13,000 into the Court Clerk's fund. On November 12, 2014, Laura Johnson filed a "Certificate of Release" with the Court Clerk's office, that represented the judgment obtained through the foreclosure on the Shorters' property had been released by Judge

Bryan C. Dixon. A copy of this document also was filed with the Oklahoma County Clerk's Office.

55. On January 23, 2015, the mortgage company filed a motion to set aside the Certificate of Release as a sham legal process conducted by Laura Johnson. On February 19, 2015, Laura Johnson filed an affidavit, as an authorized representative of Help and Hope LLC, admitting she had filed the Certificate of Release. She asserted what occurred was just a misunderstanding of the process and not an attempt to commit a fraud. Additionally, she claimed the Shorters had given Help and Hope LLC, a Power of Attorney on January 1, 2014, to handle the payment of any claim held by a mortgage. She also claimed Help and Hope LLC had a prior business and personal relationship with Joe Shorter.

56. Oklahoma County District Court Judge Dixon set aside the Certificate of Service and ordered it expunged from the records of the Oklahoma County Clerk's Office. At a subsequent sheriff's sale, the property was sold for \$75,100 to a different company.

Ongoing Warranty Deed Fraud Activity

57. I believe this warranty deed fraud is ongoing based upon a March 6, 2018, filing of a "corrected" warranty deed on the property of Jimmie G. Perkins at 5846 N. Mueller Avenue in Bethany. Based upon public records, I believe Jimmie G. Perkins died on December 8, 2010. The initial warranty deed, filed June 6, 2017, listed Perkins in Oklahoma County. I believe individuals involved in this warranty deed fraud "corrected" the initial warranted deed because notary Christi S. Cina, whose signature and notary seal

appeared on the initial deed, filed a notice on June 14, 2017, stating that her signature on the deed was a forgery.

58. The “corrected” warranty still transferred Perkins’ property to OT LLC, however, it listed Perkins as being in Denton County, State of Texas. The name and seal of Texas notary Frankie Taylor appears on this “corrected” deed. After reviewing the “corrected” deed, Frankie Taylor told investigators she did not sign or notarize the deed.

59. During the course of this investigation, I have discovered many similarities such as the use of forged and fictitious documents, forged signatures of property owners on documents, forged signatures and seals of notaries, the creation of what appear to be fictitious people and companies and the use of private postal boxes. I believe many documents such as warranty and quit claim deeds, power of attorney forms, court pleadings, affidavits and even the Bartrug’s Last Will and Testament, among other items used in this scheme are fraudulent and most likely were created on a computer.

60. For instance, fictitious mortgages were filed on four properties taken over in this warranty deed scheme. Three of the mortgages listed the mortgage holder as “The Texas Bank” while a fourth mortgage listed the mortgage holder as the “First National Texas Bank.” The language in each of these mortgages is very similar.

61. Based upon my examination of these documents, I believe a single mortgage document was created by individuals involved in this warranty deed fraud and then that document was altered each time a mortgage was filed on a different property.

62. For instance, on June 12, 2017, a fictitious mortgage with “The Texas Bank” was filed on the home of Jennifer Riggs in Marshall County which had been fraudulently

taken over in this scheme. This document directed the Marshall County Clerk to mail the mortgage, after filing, to Duende Management LLC, at 12101 N. MacArthur #A271, Oklahoma City, Oklahoma. This is an UPS store that offers private postal boxes. This postal box was opened by Cheryl Ashley on May 14, 2015. The UPS agreement authorized the delivery of mail to the postal box on behalf of Nia Forte, Duende Management, Innovative Transformation, and Help and Hope LLC. The postal box application form listed Laura Johnson as an officer of the corporation.

63. Two additional mortgages between “The Texas Bank” and Helping Hand LLC, were filed one minute apart in the Oklahoma County Clerk’s Office on February 14, 2017. These mortgages were filed against the homes of Lucinda Giovanni and Justin Weems. The language in each of these documents is very similar to the mortgage filed against Riggs. This similarity even included the uncorrected language in the mortgages that Giovanni’s and Weems’ properties were located in Marshall County when in fact they are located in Oklahoma County.

64. Finally, the mortgages filed against Giovanni’s and Weems’ properties listed the address for the Texas Bank as 5830 NW Expressway #178, Oklahoma City, Oklahoma, which is a private postal box opened June 27, 2017, by Cheryl Ashley. These two mortgages also had the forged signature and seal of notary Mitzi Norton on each document.

65. This same mortgage form appears to have been used in the fraudulent filing of a mortgage between Rejuvenation, LLC and the First National Texas Bank on the home of Tony and Becky Hawkins at 13200 Cedar Bend Dr., in Oklahoma City. The mortgage form had been changed to show the location of the property as being in Oklahoma County

rather than Marshall County. The first page of the mortgage document correctly listed the address of the Hawkins' home as 13200 Cedar Bend Dr., Oklahoma City; however, the third page of the mortgage listed the property's address as being 10204 Major Ave., The Village, OK 73120, which is actually the street address for Lucinda Giovanni's home.

66. During the course of this investigation, I have determined that some of the properties taken over or attempted to have been taken over have had the locks to the homes changed. Additionally property from within the homes had been removed and some repairs and/or renovations had been performed on the homes.

67. During the course of this investigation, I have also determined that the names of a number of different entities and companies have been used on various documents involved in this warranty deed fraud. A number of the deeds and other documents filed with county officials appear to be signed by individuals as "managing members" of these entities. I have not been able to determine if the individuals, whose names appear on these documents, actually exist.

68. During the course of this investigation, I have also determined that a number of documents filed of record in county offices in Oklahoma County and Marshall County were personally delivered by the participants in this warranty deed fraud as well as by a minor relative of the participants.

69. During the course of this investigation, I have identified phone numbers used by participants in this warranty deed fraud including Cheryl Ashley's phone (405) 388-0683 and Laura R. Johnson phone (405) 641-4016. Additionally, I have learned that Laura

R. Johnson has obtained nine prepaid cellular phone numbers from AT&T. These phone numbers are in addition to the Verizon phone number opened in the name of Jewel Bartrug.

70. During the course of this investigation, I have learned that documents filed with the Oklahoma County Clerk's Office such as warranty and quit claim deeds are electronically scanned and uploaded to a website that is accessible to the public through the Internet. Only employees of the Oklahoma County Clerk's Office and the Oklahoma County Assessor's Office have the ability to input documents into the system.

71. On 4-20-18, The Hon. Gary M. Purcell, United States Magistrate Judge, issued search warrants for two locations:

- a. No. M-203-P, authorizing a search of 8033 NW 124th Street, Oklahoma City, OK, which is the residence of Laura R. Johnson and Thomas C. Johnson Sr.;
- b. No. M-18-204-P, authorizing a search of 7313 NW 125th Street, Oklahoma City, OK, which is the residence of Cheryl M. Ashley.

72. These warrants were served on April 11, 2018. Among the items seized from Laura Johnson's house was an iPhone with telephone number (405) 641-4016. I have reviewed telephone records from AT&T which show this phone number belongs to Laura Johnson at 8033 NW 124th Street, Oklahoma City, OK, and lists the subscriber's contact email address as ljohnson143@gmail.com. This phone was searched pursuant to the search warrant described in Paragraph 71(a).

EMAIL ACCOUNTS TO BE SEARCHED – GOOGLE, INC.

73. I seek a warrant to search the content of and other information about the following email accounts from Google:

a. cashley246@gmail.com

b. ljohnson143@gmail.com

c. niaforte360@gmail.com

There is probable cause to believe that these accounts are associated with Cheryl Ashley, Laura Johnson, and the name Nia Forte, and probable cause to believe that the content of and other information about these email accounts will contain evidence of the scheme described in this Affidavit.

74. There is probable cause to believe that the requested content of and information about these email accounts will be found at premises owned, controlled, maintained, or operated by Google, Inc. All of these email accounts end in “@gmail.com.” I know from my training and experience that gmail is a free email service controlled and hosted by Google, Inc., which is headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

75. I believe email account cashley246@gmail.com belongs to Cheryl Ashley. This is based upon a filing with the Oklahoma Secretary of State for Hope and Help LLC which lists Cheryl M. Ashley, 12101 N. MacArthur Blvd, A271, email – cashley246@gmail.com as the company’s registered agent. In addition, I have reviewed a Tinker Federal Credit Union account application dated September 1, 2017 in the name of Cheryl M. Ashley. In this application, she lists her email address as cashley246@gmail.com

76. I believe email account ljohnson143@gmail.com belongs to Laura Johnson. I have searched iPhone described in Paragraph 72 of this Affidavit. When attempting to

access email from this phone, the user is prompted to log in to email using the password for the account ljohnson143@gmail.com.

77. I believe the name “Nia Forte” is an alias being used in this scheme, and that the email address niaforte360@gmail.com has been used in this scheme. As described in Paragraph 20 of this Affidavit, the letter to Lucinda Giovanni from Help and Hope, Inc., was signed by “Nia Forte,” and provided her contact email address as niaforte360@gmail.com. Further, during the search of Laura Johnson’s home at 8033 NW 124th Street, agents discovered the “Nia Forte” letter to Lucinda Giovanni described in Paragraph 20 of this affidavit. Agents also found at least two items of mail addressed to “Nia Forte” at Laura Johnson’s address, 8033 NW 124th Street, Oklahoma City, OK. As described in Paragraph 62 of this Affidavit, “Nia Forte” was authorized to receive mail at the UPS store mailbox opened by Cheryl Ashley.

78. In addition, an outgoing text message from Laura Johnson’s phone dated July 7, 2016 reads: “I need a picture of you to put on the venture pass - take a face picture of you, Elena, tanner & Conner & email to niaforte360@gmail.com.” I know from this investigation that these are the names of the children of Laura Johnson’s brother, Raymond.

79. I believe there is probable cause that the email accounts described in this affidavit were used to perpetuate this scheme. I have reviewed many hundreds of pages of text messages found on Laura Johnson’s phone, described in Paragraph 72, and have found numerous references to using email in connection with this scheme. Examples include:

a. On 6-11-2015, a text message from Marri Nevarez to Laura Johnson reads: “Hey Laura! Hope you're doing well haven't talked to you in a while sorry! I've been

distracted a lot has happened for me over here lol. But Mike has been helping me with finding houses and I think we might have one I'll email you the details of it.”

b. On 6-21-15, a text message from Laura Ashley to Mike Elias and Marri Nevarez states “Did you guys go look inside this house? I show it was bought in 2012 for 225,000.00 then they supposedly spend 300k to update property. The taxes were in default thru 2013 & they just paid them up to date last week Not sure if any liens on property but put in an email. Are there any homes in that area that are vacant? If so send me those addresses to please!:)”

c. On 7-16-2015 an outgoing text message from (405) 641-4016 reads: “This on is bidding online so I'm good on that for now. I might hire him to project manage or fix some things if he wants to. When I switched to my new phone it didn't transfer his info because I didn't back it up to iCloud first smh I have his info on my old phone & can look it up!:) did you get the email for notary stuff etc?”

80. I believe the email account ljohnson143@gmail.com was used in this scheme. I have reviewed text messages found on the iPhone. One series of communications is between ljohnson143@gmail.com and a subcontractor for Lumber Liquidators. In this exchange, it appears that the subcontractor contacted Laura Johnson by email at ljohnson143@gmail.com, after which she responded by text message from phone number (405) 641-4016. This exchange included the following messages from Laura Johnson on June 27, 2015:

a. “I have 2 properties for you to bid. One is the upstairs of my house & one is a rental property in warr acres about 15min from my house.”

b. “Do you just install wood floors or do you do other work as well? I may need a cpl other quotes if you paint or do other work with fixing up houses?”

c. After discussing their schedules, the subcontractor asked “Can I get your last name please.” The response reads, “Yes that will work. Laura Johnson is the name :)”

d. On June 28, 2015, an outgoing message from (405) 641-4016 reads: “I gave them my home address – which is different than the rental – but would like to do the rental first & then go from there if I like the job.”

81. Additional information showing that these email addresses and others were used in the scheme was found on a computer belonging to Tom Johnson, which was seized and searched pursuant to the warrant for his residence. This computer was found in Tom Johnson’s home office; was identified by Tom Johnson as belonging to him; and Tom Johnson provided agents with the computer’s password. The following are examples of emails found on the computer which establishes that these email accounts were used in the scheme:

a. On 1/29/2015, Nia Forte sent an email from niaforte360@gmail.com to Thomas Johnson at tjohnsontsg@me.com which included a Limited Power of Attorney between Joe Shorter and Janice Shorter to appoint Help and Hope LLC as true and lawful attorney to pay or claim funds currently held by any mortgage or government agency. This form is unsigned and not notarized.

b. On 11/21/2016, Thomas Johnson sent an email from tjohnsontsg@icloud.com to niaforte360@gmail.com and Laura Johnson at ljohnson143@gmail.com. Attached to this email was a .pdf file for Innovative

Transformations Inc Business Plan – 2016 in which it states “so far our firm has only purchased tax lien properties” and includes the Innovative Transformations Estimated Profits 2017 sheet with 8 properties listed. As noted above in Paragraphs 38 and 39, Innovative Transformations was used in the takeover of the Jewel Bartrug property.

c. Also on 11/21/2016, Thomas Johnson sent an email from tjohnsontsg@icloud.com to Nia Forte at niaforte360@gmail.com with the Innovative Transformations Business Plan - Revision #2.

d. On 11/29/2016, Thomas Johnson sent an email from tjohnsontsg@me.com to Cheryl Ashley at cashley246@gmail.com. Attached was a .pdf file with Innovative Transformation – Estimated Profits 2017. It included eight properties including three in Warr Acres.

e. On January 17, 2017, Thomas Johnson sent an email from tjohnsontsg@icloud.com to Cheryl Ashley at cashley246@gmail.com, which read: “YO MOLDY – OLDY CHICK: New spreadsheet attached. MAKE SURE YOU KNOW THIS FRONT TO BACK YOU JERK!!! All of the information you were asking for was in the old one anyway.” Attached to this email was a .pdf file showing Innovative Transformations 2016 Information and Estimated Profits 2017, which lists nine properties: four in Warr Acres, one in Nevada, one in The Village, two trailers in Jones, and one at 9th Street Property.

f. On 2/1/2017, Nia Forte sent an email from niaforte360@gmail.com to Thomas Johnson at tjohnsontsg@icloud.com with a subject line of “Print Please” which included a hyperlink to a web page at oklaw.org concerning general appearance waiver of

summons. Also attached was a .pdf blank copy of General Appearance and Waiver of Summons for Oklahoma State District Court.

g. On 2/22/2017, an email was sent from niaforte360@gmail.com to tjohnsontsg@me.com. This was a forwarded email to Laura Johnson at ljohnson143@gmail.com that contains a .pdf from Antero Oil and Gas Lease for the Estate of Jewel M. Bartrug by Laura Johnson, Executrix.

h. On 2/26/2018, niaforte360@gmail.com sent an email to tjohnsontsg@me.com regarding building permits in Warr Acres with a hyperlink to www.warracres-ok.gov.

i. On 3/28/18, an email was sent from niaforte360@gmail.com to Thomas Johnson at tjohnsontsg@me.com which contained a forwarded email message from Laura Johnson at ljohnson143@gmail.com to niaforte360@gmail.com, forwarded again from Antero Oil and Gas Lease. The email is from Antero stating they are cutting a check to Laura Johnson and asking her to sign the attached ratification as a final curative document to ratifying the lease from the Jewel M. Bartrug Estate.

82. I believe that emails sought in this warrant application are still located at Google, Inc. A preservation request was sent on April 11, 2018 and an extension of this request was sent on July 11, 2018. Another extension was sought by letter on October 11, 2018.

83. In addition, I know from my training and experience that in general, an email sent to a Google, Inc. subscriber is stored on the subscriber's "mailbox" on Google, Inc. servers until the subscriber deletes the email. If the subscriber does not delete the email,

the message can remain on the email provider's servers indefinitely. And even if the subscriber deletes the email, it may continue to be available on Google, Inc. servers for a certain period of time.

EMAIL AND/OR iCloud ACCOUNTS TO BE SEARCHED – APPLE, INC.

84. I also seek a warrant to search the content of and other information about the following email account and iCloud accounts from Apple, Inc.:

- a. tjohnsontsg@me.com
- b. tjohnsontsg@icloud.com
- c. niaforte360@icloud.com
- d. any iCloud account associated with:

Laura R. Johnson
8033 NW 124th Street
Oklahoma City, OK 73142-2232
Telephone number (405) 641-4016

INFORMATION REGARDING APPLE ID AND iCloud¹

85. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at <https://support.apple.com/kb/PH26502>.

86. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.
- d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations,

spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
- f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.
- g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.
- h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through

iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

87. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

88. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

89. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account

(including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

90. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

91. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services

through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

92. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

93. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus

enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

94. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

95. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

96. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information

on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

97. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

98. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

**iCLOUD ACCOUNTS AND EMAIL ACCOUNTS
TO BE SEARCHED – APPLE, INC.**

99. I believe there is an iCloud account associated with Laura Johnson, and that this account will contain evidence of the offenses described in this affidavit.

a. I have examined Laura Johnson's phone, which was taken during the search warrant served at her home. A review of the user-configured settings on this phone shows that it is configured to perform a full backup of the phone to an iCloud

account. The text message described in Paragraph 79(c) of this affidavit demonstrates that Laura Johnson is aware of and utilizes this backup feature.

b. My examination of Laura Johnson's phone shows that it contains a large number of photographs pertaining to this scheme. Examples include photos of a number of houses; photos of Notices of Violations posted at several houses, photos of an individual's appointment as a notary; screenshots of a web page on Justitia.com describing transferring real property; a number of screenshots of property lists maintained at oklahomacounty.org; screenshots of searches for the name "Bartrug"; photos of letters testamentary for Jewel M. Bartrug; a photo of a death certificate for Jack Bartrug; an incorporation agreement for Innovative Transformations, giving Cheryl Ashley 80 percent and Laura Ashley Johnson 20 percent; screenshots of wills, trusts, liens, tax rolls, quitclaim deeds, tax statements, unclaimed property, and other documents or searches pertaining to property. As described above, the iCloud account is likely to contain backups of this data from this phone as well as data from or shared with other Apple devices.

100. I believe there is an Apple email account and iCloud account associated with Tom Johnson and that this account will contain evidence of the offenses described in this affidavit. As shown in Paragraph 81 above, emails pertaining to this scheme were sent from and to tjohnsontsg@icloud.com and tjohnsontsg@me.com. As explained above, these email domains are hosted and controlled by Apple, Inc. Email messages from and to both accounts were found on Tom Johnson's computer. In addition, both email addresses were

used to send documents pertaining to Innovative Transformations, a company known to have been used in the scheme.

101. Further, I have reviewed email header information, provided by Google, Inc., dating back to January, 2014. This information does not include email content, but does show the date, time, email addresses of the sender and recipient, and other technical information. These records show that emails were sent to cashley246@gmail.com from tjohnsontsg@icloud.com on 1-3-2017 and 1-17-2017.

102. I believe there is an iCloud account associated with the name Nia Forte and that this account will contain evidence of the offenses described in this affidavit. This is based upon my review of email header information provided by Google, Inc. My review of this information showed the following:

a. Emails were exchanged between “niaforte360@icloud.com” and “cashley246@gmail.com” on 11-21-2016, 1-3-2017, 1-4-2017, 2-6-2017, 2-16-2017, 2-17-2017, and 4-1-2017.

b. Numerous emails were exchanged between “niaforte360@icloud.com” and “ljohnson143@gmail.com” between 10-12-2016 and 2-1-2018.

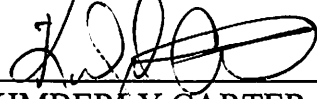
c. As described above, it appears that “Nia Forte” is an alias associated with Laura Johnson, and used extensively in this scheme. “Nia Forte” purportedly signed the letter to Giovanni from Help and Hope, Inc. as described in Paragraph 20, and was purportedly a witness to the Jewel Bartrug will as described in Paragraph 41.

103. I believe there is probable cause that iTunes account information will contain evidence of the scheme. As described in Paragraph 45 of this affidavit, Thomas C. Johnson,

Sr., is listed as the CIO of TSG Enginuity, Inc, which is associated with the address of 8033 NW 124th, Oklahoma City. This is the home address of Laura Johnson and Thomas C. Johnson Sr. I have reviewed bank statements for TSG Enginuity, Inc. for the time period from January, 2015 through June, 2016. These statements show a large number of payments to iTunes, often in large, consistent dollar amounts, within a short period of time. For example, on February 2, 2015, there were five payments to iTunes, each in the amount of \$99.99. On February 5, 2015, there were five payments to iTunes, each in the amount of \$99.99. In the month of July, 2015, there were approximately 37 payments to iTunes. Most were for \$99.99, although the amounts ranged from \$24.99 to \$307.98. Similar iTunes purchase history appears throughout these bank statements for the time period described above. I know from my training and experience that gift cards or account balances that can be converted to gift cards or stored value cards are a common method for moving or transferring money anonymously.

CONCLUSION

104. I submit that this affidavit supports probable cause for a warrant to search the premises described in Attachment A and seize the items described in Attachment B.



 KIMBERLY CARTER
 Special Agent
 United States Secret Service

Subscribed and sworn to before me this 9th day of November, 2018.



 GARY M. PURCELL
 United States Magistrate Judge

ATTACHMENT A

PLACE TO BE SEARCHED

This warrant applies to content of and information about the following accounts:

- a. tjohnsontsg@me.com
- b. tjohnsontsg@icloud.com
- c. niaforte360@icloud.com
- d. any iCloud account associated with:

Laura R. Johnson
8033 NW 124th Street
Oklahoma City, OK 73142-2232
Telephone number (405) 641-4016

that are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

A handwritten signature in black ink, appearing to be "JLB" with a flourish underneath.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc., regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that have been deleted but are still available to Apple, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. The contents of all emails associated with the accounts from January, 2014 until April, 2018, including stored or preserved copies of emails sent to and from the accounts (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each

A handwritten signature in black ink, located in the bottom right corner of the page. The signature is stylized and appears to be written in cursive.

email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

c. The contents of the following files and other records stored on iCloud: all iOS device backups, and all files and other records related to iCloud Mail.

d. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including mail logs, iCloud logs, and iTunes Store logs.

e. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

f. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Handwritten signature in black ink, appearing to read "amb Kwan".